

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO**

UNITED STATES OF AMERICA

Plaintiff,

v.

Case No. 1:16-CR-4571 JCH

GUY ROSENSCHEIN,

Defendant.

**DEFENDANT DR. ROSENSCHEIN'S OBJECTIONS
TO THE MAGISTRATE JUDGE'S PROPOSED FINDINGS AND
RECOMMENDED DISPOSITION [DOC.183]**

Defendant Dr. Guy Rosenschein, by and through counsel of record, Marc M. Lowry of Rothstein Donatelli LLP, hereby objects to United States Magistrate Judge Jerry H. Ritter's Proposed Findings and Recommended Disposition [Doc. 183] (hereinafter "Order") in this matter. In his Order, Magistrate Judge Ritter recommends that Microsoft Corporation's Motion to Modify Rule 17(c) Subpoena [Doc. 125] be granted and that Dr. Rosenschein's request for a hearing [Doc. 141] be denied. Dr. Rosenschein objects to the lower court's legal analysis for the following reasons:

INTRODUCTION

Dr. Rosenschein objects to and seeks review of the United States Magistrate Judge's Proposed Findings and Recommended Disposition on Microsoft's Motion to Modify Rule 17(c) subpoena [Doc. 125] and his denial of defendant's request for a hearing [Doc. 141]. These objections are filed under 28 U.S.C. § 636(b)(1)(C) and Federal Rule of Criminal Procedure 59(a) which provide de novo review of a Magistrate's findings and recommendations. Judge Ritter's Order proposes that the Court find that the subpoena directed at Microsoft is not sufficiently specific. Doc. 183 at 10. Alternatively, the Order recommends the Court find that the

subpoena is oppressive. *Id.* at 12. The Order further recommends that the Court deny Dr. Rosenschein’s request for a hearing. *Id.* Dr. Rosencheim respectfully requests the Court set aside these findings and recommendations.¹

APPLICABLE LAW

Materials may be reached under Fed. R. Crim. P. 17(c) “as long as they are evidentiary.” *Bowman Dairy Co. v. United States*, 341 U.S. 214, 219 (1951). Rule 17(c) “establish[es] a more liberal policy for the production, inspection and use of materials at the trial.” *Id.* at 220. *United States v. Nixon*, 418 U.S. 683 (1974), requires that the requested materials be evidentiary and relevant, and that the requesting party show the subpoenaed materials are relevant, admissible, and specific. *Id.* at 699-700. In *Nixon*, the Supreme Court explicitly declined to decide how strongly the evidentiary requirement applies to subpoenaed materials possessed by third parties. *Id.* at 699 n.12.

“The right to the production of all evidence at a criminal trial . . . has constitutional dimensions.” *Nixon*, 418 U.S. at 711. “It is the manifest duty of the courts to vindicate those [constitutional] guarantees, and to accomplish that ***it is essential that all relevant and admissible evidence be produced.***” *Id.* (emphasis added). Rule 17(c) is based on the accused’s Due Process Rights and his Sixth Amendment Right to Compulsory Process. *United States v. Tomison*, 969 F.Supp. 587, 593 (E.D. Cal. 1997). “Rule 17(C) implements the Sixth Amendment guarantee that an accused have compulsory process to secure evidence in [his] favor.” *United States v. Winner*, 2018 WL 1998311, at *2 (S.D. Ga. Apr. 27, 2018) (unreported) (internal quotation marks and citation omitted).

¹ Dr. Rosenschein incorporates by reference the arguments and exhibits made in his earlier filings on this issue.

A. Dr. Rosenschein's Rule 17(c) requests as narrowed in the by the parties' negotiations were sufficiently specific and discoverable.

Judge Ritter's Order proposes that the Court find that Dr. Rosenschein has not demonstrated sufficient specificity in his subpoena to Microsoft. *See* Doc. 183 at 10. While specificity may be the "most difficult hurdle to overcome," *United States v. Wittig*, 247 F.R.D. 661, 663 (D. Kan. 2008) (internal citation omitted), when viewed in light of the fact that the subpoena at issue is directed to a third party, the subpoena is sufficiently specific. Federal courts have noted that a "real question remains as to whether it makes sense to require a defendant's use of Rule 17(c) to obtain material from a non-party" to satisfy the same specificity standard that applies to the government. *United States v. Nachamie*, 91 F.Supp.2d 552, 562 (S.D.N.Y. 2000). Several Courts, including Courts within this District, have found that the standard articulated in *Nixon* for specificity under Rule 17(c) subpoenas is lower for third parties than it is for subpoenas directed to the government. *See, e.g., United States v. Grobstein*, 2013 WL 12334156, at *3 (D.N.M. Apr. 26, 2013) (Vazquez, J.) (unreported). Judge Ritter's Order suggests that the standard employed by the Court in *United States v. Nosal*, 293 F.R.D. 403, 409 (N.D. Cal. Mar. 1, 2013) and relied on by Dr. Rosenschein is "contrary to the *Nixon* standard" and "the minority view." Doc. 183 at 10 n. 1. However, in *Grobstein*, the District Court of New Mexico found that a more liberal standard for subpoenas directed to third parties "is, in fact, consistent with Supreme Court precedent." 2013 WL 12334156, at *3. Additionally, *Nosal* is merely one of many District Courts to refrain from reading into Rule 17(c) terms or words that are not written there and chose to apply "the standard contained in Rule 17(c) itself." Hence, as Rule 17(c) applies to third parties, the standard is whether the subpoena is reasonable and "not unduly oppressive for the producing party to respond." *Nachamie*, 91 F.Supp.2d at 563. Federal Courts have long noted the distinction between subpoenas directed to governmental entities and those directed to third parties. For instance,

[T]he ‘specificity’ prong of the *Nixon* test is somewhat more complicated if Rule 17 is a way for a defendant to obtain documents relevant to his defense without knowing exactly what the documents are. In the context of a subpoena to the government, whom Rule 16 already requires to turn over any item that is material to preparing the defense . . . the ‘specificity’ prong makes sense because its function is to prevent the exception from . . . swallowing the rule.

United States v. Rajaratnam, 753 F.Supp.2d 317, 320 at n.1 (S.D.N.Y. 2011) (quoting *United States v. Stein*, 488 F.Supp.2d 350, 366 (S.D.N.Y. 2007)). However, when such a subpoena is directed to a third party the specificity concerns addressed in *Nixon* substantially fade.

To read Rule 17(c) with equal stringency with respect to third parties and the Government, would contravene the purpose of the rule’s more liberal policy. It would prevent criminal defendants from accessing evidence that is material to their defense, and it could even create a perverse incentive for the Government not to obtain potentially exculpatory material from third parties.

Grobstein, 2013 WL 12334156, at *3.

Judge Ritter’s Order relies heavily on the Court’s findings in *United States v. Wittig*, 247 F.R.D. 661 (D. Kan. 2008). It is important to note, however, that the *Wittig* Court, in a subsequent ruling, found that a “request will usually be sufficiently specific where it limits documents to a reasonable period of time and states with reasonable precision the subjects to which the documents relate.” 250 F.R.D. 548, 552 (D. Kan. 2008). Moreover, “in the context of a subpoena to a third party to whom Rule 16 does not apply, requiring the defendant to specify precisely the documents he wants without knowing what they are borders on rendering Rule 17 a nullity.” *Rajaratnam*, 753 F.Supp.2d at 320 n.1. Dr. Rosenschein satisfied the Rule 17(c) standard for third parties, especially after he narrowed the scope of materials requested under the subpoena as originally drafted. See email from defense counsel to Microsoft’s counsel dated February 18, 2019 contained in Doc. 125-1, pp. 66-68; cf. *Democratic National Committee v. McCord*, 356 F.Supp. 1394, 1396 (D.D.C. 1973) (holding that the “fact that the materials

requested cover an extended period of time and are voluminous will not render the subpoenas invalid”).

In proposing that the Court find that Dr. Rosenschein has not demonstrated sufficient specificity, Judge Ritter suggests that the subpoena directed at Microsoft reads as a civil “discovery request.” *See* Doc. 183 at 9-10. It is critical to note, however, that “Rule 16 provides no mechanism to inspect documents or other items that are not in the Government’s possession.” *Grobstein*, 2013 WL 12334156, at *3. For example, the

notion that because Rule 16 provides for discovery, Rule 17(c) has no role in the discovery of documents can, of course, only apply to documents in the government’s hands; accordingly, Rule 17(c) may well be a proper device for discovering documents in the hands of third parties.

Tomison, 969 F.Supp 587 at n. 14 (quoting *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951)) (internal alteration omitted). This discovery standard has been extended by other Courts as well.

Because Rule 16 only addresses discovery between the parties, if defendants seek documents from non-parties, it must be pursuant to some other rule. If this were not the case, the government could prevent defendants from obtaining material by choosing not to obtain it for itself. This perverse result cannot be intended by the Federal Rules of Criminal Procedure.

United States v. Tucker, 249 F.R.D. 58, 65 (S.D.N.Y. 2008). So the Magistrate Judge was wrong to suggest that Rule 17(c) is not a discovery device; it most certainly is. And when third party corporations operate in secrecy and hide documents and materials from the public view it is quite

impossible to provide the level of specificity demanded by the magistrate court.² Finally, “[t]he degree to which document requests must be specified depends upon the facts and circumstances of each case.” *Cf. United States v. International Business Machines Corp.*, 83 F.R.D. 97, 107 (S.D.N.Y. 1979) (internal citation omitted).

Judge Ritter’s Order relies on decisions from the Fourth and Eighth Circuits where defendants sought to use subpoenas to establish agency between internet service providers and the government. Doc. 183 at 11. Those cases are not instructive here. As of 2016, years after the cases cited by Judge Ritter were decided, the Tenth Circuit held NCMEC is a federal law-enforcement agency; as such, NCMEC does not enjoy the private status that it may have held in the Fourth and Eighth Circuits when those cases were decided. *See Ackerman*, 831 F.3d 1292, 1296, 1300 (10th Cir. 2016).

United States v. Richardson is markedly distinct from our facts. In that case, AOL detected and transmitted suspected images of child pornography to NCMEC by use of a scanning program and hash value library, each of which AOL had developed for AOL’s exclusive use. 607 F.3d 357, 362 (4th Cir. 2010). In *Richardson* AOL had not collaborated with NCMEC or

² In this sense, it was unfair for Judge Ritter to criticize Dr. Rosenschein for not knowing the identity or the IP address of the website used to provide the CyberTip information to NCMEC in this case or the identity of individuals preparing or sending the CyberTip to NCMEC as noted in subpoena requests (c), (d), and (e). Doc. 183, p. 11. This is something only Microsoft could know, and that information is not publicly available. These subpoena requests were very specific and identified precisely the information sought by Dr. Rosenschein. Nevertheless the Magistrate Judge denied them as lacking in specificity, despite the very discrete requests. If Dr. Rosenschein knew these things, he would not have to ask for that information from Microsoft via a Rule 17(c) subpoena. But more importantly, such information is material and relevant to the agency issue because Dr. Rosenschein needs to show that Microsoft is responsible for the CyberTips sent from an electronic address associated with Microsoft, and that NCMEC was well aware of the actual source of the information. Likewise, the Magistrate Judge wrongly suggested that the CyberTips “were generated by Chatstep,” Doc. 183, p. 3, when Microsoft has acknowledged that the PhotoDNA software it hosted on Microsoft’s cloud service creates the purported hash match and then collected information provided by Chatstep on Microsoft’s “Reporting API” before Microsoft routes that information to NCMEC. Doc. 82-6, ¶¶ 11-12. The evidence requested will show that the CyberTip was “generated” by Microsoft to send to NCMEC.

any other law enforcement agency to develop the computer program or the hash value library. Richardson rejected the defendant's agency argument because the Fourth Circuit concluded that a private search occurred using AOL's "internally developed scanning programs" and hash databases. *See id.* at 362, 367. AOL then followed the statutory reporting requirements by forwarding the suspect images to NCMEC. At that time and in that Circuit NCMEC had *not* been identified as a federal law-enforcement agency. *See id.* at 360. Here, as discussed at length in Dr. Rosenschein's briefings, there is substantial evidence of collaboration between NCMEC (a federal law enforcement agency) and Microsoft in developing and implementing the PhotoDNA program to detect and report suspected images of child pornography. *See, e.g.*, Docs. 71, 74, 77, 85, 86, 108, & 136. Hence *Richardson* the opposite this case.

Likewise, in *United States v. Stevenson*, the defendant argued that AOL acted as a government agent by intercepting suspected images of child pornography through the scanning software it developed entirely on its own (and using AOL's unique, internally-developed hash value library) and by following the statutory requirement to report the images to NCMEC. 727 F.3d 826, 829-30 (8th Cir. 2013). In contrast to this case, *Stevenson* noted that AOL "operates its file-scanning program *independently* of any government program designed to identify . . . images of child pornography." *Id.* at 830-31 (emphasis added). Here, of course, Microsoft relied on NCMEC not only for the original set of child pornography images to develop PhotoDNA and the original hash value library, but Microsoft continues to rely on NCMEC to constantly provide the PhotoDNA program with hash values to use. Additionally, *Stevenson* relied on the fact that the defendant offered no evidence that "the government knew of and acquiesced in the search, and that AOL conducted the scan to assist law enforcement." *Id.* at 830. That presentation stands in stark contrast to what Dr. Rosenschein has shown here by providing substantial evidence that NCMEC and Microsoft collaborated in developing the PhotoDNA program in order to intercept

suspected illicit images so they could be reported to law enforcement for prosecution. There exists substantial, critical evidence of knowledge and acquiescence in this case that requires and supports the production of the subpoenaed materials. The subpoenaed materials are relevant and material to the legal issues to be resolved in this case. Furthermore, the Court in *Stevenson* noted that the defendant did not argue that a more liberal standard should apply to a subpoena directed to a third party as Dr. Rosenschein has done here. *Id.* at 831.

B. A Sampling of The Subpoena Requests That Were Wrongly Denied.

(b) This subpoena request sought all communications sent from Microsoft to NCMEC on Chatstep's behalf concerning any user with the moniker "Carlo" from July 25, 2016 to August 10, 2016 addressed in the two specific CyberTip reports in this case. This request also included all electronic data that Microsoft provided to NCMEC concerning those two CyberTipline reports. Despite the specificity of this request, the Magistrate Judge denied it.

(c) This subpoena request sought the URL used by the Microsoft PhotoDNA service that provided NCMEC with information concerning the two CyberTipline reports in this case. Despite the specificity of this request that was limited in time, the Magistrate Judge denied it.

(d) This subpoena request sought the IP address or email address used by Microsoft to forward data concerning the two CyberTipline reports in this case to NCMEC. Despite the discrete and specific request limited in time, the Magistrate Judge denied it.

(e) This subpoena request sought the identity of the person or computer program that forwarded the data associated with the CyberTipline reports in this case to NCMEC.

Despite the specificity and the limited time frame associated with this request, the Magistrate Judge denied it.

(l) The subpoena request sought documentation of the specific hash value matches that were associated with the two CyberTipline reports in this case, including the name of the hash value set (or library) that was used to make the match as well as the actual hash value and the hash match number. Despite the specificity of this request, the Magistrate Judge denied it.

(m) The subpoena request sought all communications involving Microsoft addressing the two CyberTipline reports in this case, including the original data transfer that Microsoft made to NCMEC concerning the two CyberTipline reports in this case. Despite the specificity of the request (focusing only on communications involving these two CyberTipline reports), the Magistrate Judge denied it.

(n) The subpoena request sought communications addressing assistance that Microsoft may have offered or provided to two NCMEC employees who presented a lecture to prosecutors and law enforcement officers discussing the Tenth Circuit's decision in *U.S. v. Ackerman* during the 2017 Crimes Against Children Conference. Despite the discrete and specific request for information, the Magistrate Judge denied it.

(o) The subpoena request sought communications between Microsoft and NCMEC addressing NCMEC's PhotoDNA Initiative. Despite the specific request for communications about an Initiative that is known to exist, the Magistrate Judge denied it.

(q) The subpoena request sought correspondence between Microsoft and NCMEC addressing NCMEC's ability to use the PhotoDNA program and sublicense the

PhotoDNA program to third parties. Despite the specificity of this request, the Magistrate Judge denied it.

(r) The subpoena request asked for correspondence with any law enforcement agency or officer concerning the two CyberTipline reports made in this case. Despite the specificity of this request, the Magistrate Judge denied it.

C. Dr. Rosenschein's requests, especially as narrowed, are not oppressive.

Judge Ritter also suggests that compliance with the subpoena would be oppressive. *See* Doc. 183 at 12. In *Nixon*, the Court held that “[a] subpoena for documents may be quashed if their production would be unreasonable or oppressive, but not otherwise.” 419 U.S. at 698 (internal quotation marks omitted). “[T]he burden of production must be compared to the size of and available resources of the responding party.”³ *International Business Machines Corp.*, 83 F.R.D. at 108. Judge Ritter’s Order takes issue with the authority cited by Dr. Rosenschein in his response to Microsoft’s motion [Doc. 136 at 22] because the matters in question in those cases took place in the context of grand jury investigations. Doc. 183, p. 12. The grand jury cases are relevant, of course, because “[u]nlike the Government, the defendant has not had an earlier opportunity to obtain material by means of a grand jury subpoena.” *Nachamie*, 91 F.Supp.2d at 562-63. Even still, Courts have made clear that the graver concerns of our legal system to provide for constitutional due process protections for a criminal defendant transcends the burdens a subpoena may impose on a third party. For example, in antitrust actions federal courts have found that:

[i]nconvenience is relative to size. Any witness who is subpoenaed suffers inconvenience. An individual operating a small business, for example, or a corporation operated by a sole shareholder, may suffer, in like circumstances,

³ As of June 30, 2019, Microsoft employs 144,106 individuals of which 85,306 are in the United States and 51,854 are in Washington State. MICROSOFT, *Facts About Microsoft*, <https://news.microsoft.com/facts-about-microsoft/#EmploymentInfo> (last visited October 10, 2019).

more inconvenience than the [corporation] with its thousands of employees. But this inconvenience, whether suffered by witnesses, grand jurors, or jurors, is part of the price we pay to secure the effective administration of justice and enforcement of our laws.

International Business Machines Corp., 83 F.R.D. at 108 (quoting *In re Radio Corp. of America*, 13 F.R.D. 167, 172 (S.D.N.Y. 1952)). The Court in *International Business Machines Corp.* further held that the burden that accompanied a subpoena duces tecum served on IBM “may be substantial on an absolute scale, [but] when compared with IBM’s size and resources it is neither unduly burdensome nor oppressive.”⁴ *Id.* at 109.

“The burden of establishing that compliance would be unreasonable or oppressive rests, of course, on the subpoenaed witness.” *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 305 (1991) (Stevens, J., concurring). Microsoft has merely asserted that the costs of compliance would be prohibitive, but has failed to provide specific evidence to support this claim. An assertion, without more, is insufficient to demonstrate that compliance with a subpoena is oppressive. *See, e.g., N.L.R.B. v. Interstate Dress Carriers*, 610 F.2d 99, 112 (3d Cir. 1979) (“[T]he burden on the party to whom the subpoena is addressed is not a meager one”); *N.L.R.B. v. Midwest Heating and Air Conditioning*, 528 F.Supp.2d 1172, 1179 (D. Kan. 2007) (noting that the burden on the resisting party “is not easily met”). In fact, even if the Court accepts Microsoft’s assertion that compliance would cost the company around one million dollars, that (overstated) figure represents less than .0008% of the company’s revenue for the fiscal year ending in June 2019, and less than .002% of its operating income.⁵ Viewed in this light and in an appropriate financial context the request is not oppressive at all.

⁴ For the fiscal year ending in June of 2019, Microsoft reported \$125.84 billion in revenue with \$42.96 billion as operating income. Dan Gallagher, *Microsoft Keeps its High Score*, WALL ST. J. (July 18, 2019 7:58PM), <https://www.wsj.com/articles/microsoft-keeps-its-high-score-11563494331>.

⁵ *See id.*

Moreover, Microsoft's cost estimate is not reflective of Dr. Rosenschein's February 18, 2019 attempt to narrow the subpoena as originally drafted, nor is this narrowing attempt adequately addressed in the corresponding sections of Judge Ritter's Order. *See* Doc. 183 at 12. In fact, Judge Ritter describes the cost of compliance as "hundreds of thousands of dollars" if the subpoena is narrowed as requested, Doc. 183, p. 8, but that figure is not sufficiently particularized in Microsoft's declarations to be reliable. The Order then suggests that "[i]f every defendant in every child pornography prosecution were to be permitted to make such requests service providers would be forced to abandon preventative efforts." *See* Doc. 183 at 12. But that is not the constitutional standard to be applied in a criminal case. Having voluntarily placed itself at the epicenter of this illegal child pornography reporting scheme by collaborating with NCMEC to develop and implement PhotoDNA, and having expended considerable financial resources to do so, Microsoft cannot now cry foul over the cost of compliance with the production of relevant and material information in a criminal case. The cost of compliance here is insignificant compared to the financial investment that Microsoft has made to provide this service for free to law enforcement agencies, ESPs, and NCMEC. Judge Ritter's contention ignores the reality that once Microsoft secures this evidence the cost of compliance for future cases seeking to prove agency due to Microsoft's relationship with NCMEC will be minimal. By no means would it impact Microsoft's ability to function as one of the world's largest corporations.

It should be noted that Judge Ritter's Order cites no authority supporting his recommendation that the subpoena is oppressive. In fact, Judge Ritter acknowledges that "Microsoft may be a company of nearly endless resources." Doc. 183, p. 12. Which is why Microsoft can afford to give away the PhotoDNA program to NCMEC, ESPs, and law enforcement agencies despite having spent millions of dollars to develop it. Quite simply, the

cost of compliance with Dr. Rosenschein's subpoena, when placed into the appropriate context, is not oppressive for this massive, well-capitalized corporation.

D. Dr. Rosenschein request for a hearing on this issue.

Dr. Rosenschein reasserts his request for a hearing to aid the Court in resolving the legal issues set forth in the briefs on the issues presented. *See* Docs. 125, 136, & 138. The availability of the parties to answer any questions concerning Dr. Rosenschein's narrowed subpoena requests could greatly assist the Court's understanding of the nuances of the issues presented.

CONCLUSION

WHEREFORE, for the reasons discussed above, Dr. Rosenschein respectfully requests that the District Court conduct a de novo review of the issues presented by Microsoft's motion and overrule the proposed findings and recommended disposition in Doc. 183. Dr. Rosenschein further requests a hearing on this matter, or, in the alternative, for the Court to order Microsoft to make available the materials requested in the subpoena to Dr. Rosenschein.

Respectfully submitted,

ROTHSTEIN DONATELLI LLP

/s/ Marc M. Lowry

MARC M. LOWRY

500 4th Street N.W., Suite 400

Albuquerque, NM 87102

(505) 243-1443

mlowry@rothsteinlaw.com

Attorney for Defendant Guy Rosenschein

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 16th day of October, 2019, I filed the foregoing pleading electronically through the CM/ECF system, which caused all counsel entitled to notice to be served by electronic means, as more fully reflected on the Notice of Electronic Filing:

Sarah Mease
United States Attorney's Office
P.O. Box 607
Albuquerque, NM 87103
sarah.mease@usdoj.gov

Mark Baker
Peifer, Hanson, & Mullins, P.A.
P.O. Box 25245
Albuquerque, NM 87125-5245
Tel: (505)247-4800
Fax: (505) 243-6458
mbaker@peiferlaw.com

Alexander A. Berengaut
Megan A. Crowley
Jadzia B. Pierce
Covington & Burling, LLP
One City Center
850 Tenth Street N.W.
Washington, DC 20001-4956
Tel: (202) 662-5367
aberengaut@cov.com
MCrowley@cov.com
JPierce@cov.com

/s/ Marc M. Lowry

ROTHSTEIN DONATELLI LLP